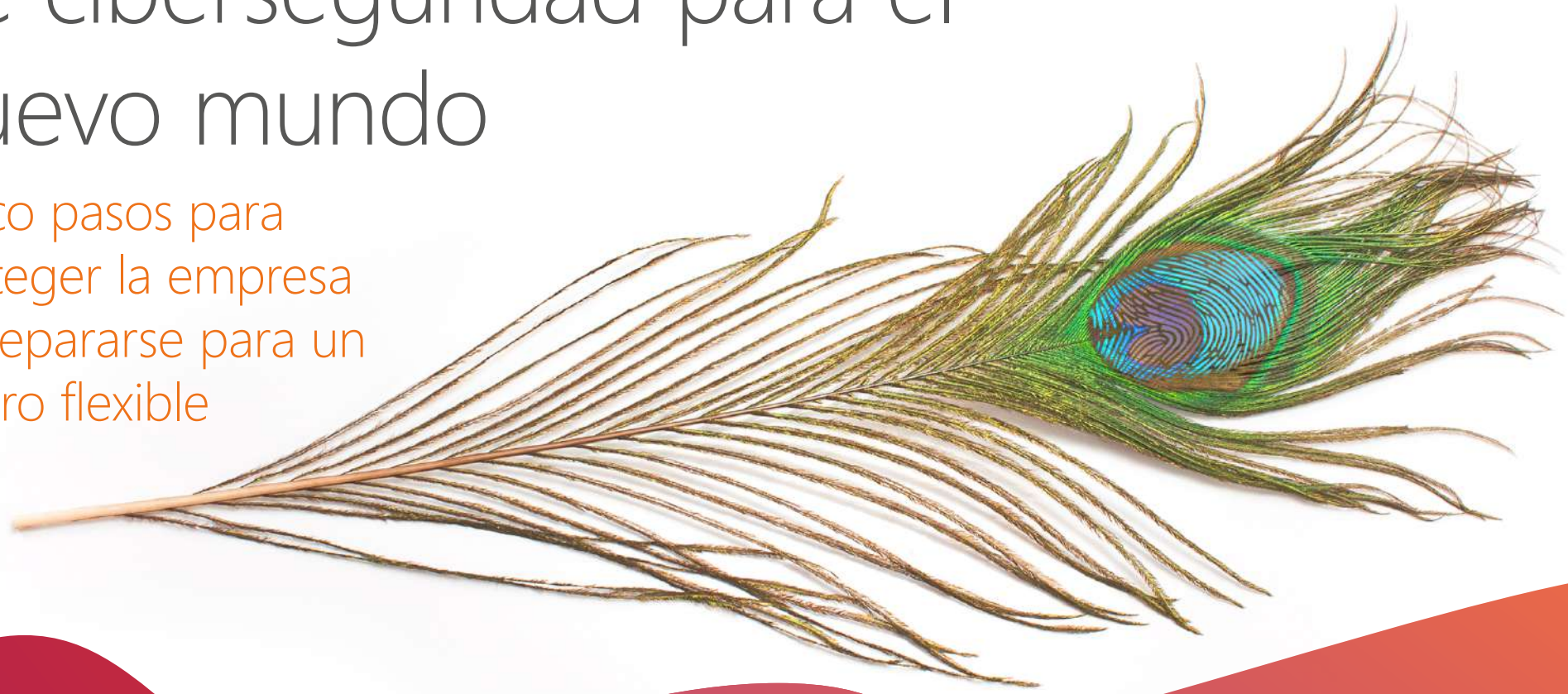
Redefina su estrategia de ciberseguridad para el nuevo mundo

Cinco pasos para proteger la empresa y prepararse para un futuro flexible



avanade

Redefina su estrategia de ciberseguridad para el nuevo mundo

No hay ninguna industria, organización o persona que no se haya visto afectada por la pandemia de COVID-19. Tanto lo que compramos como nuestra forma de vivir y trabajar han cambiado para siempre, y lo han hecho mucho más rápido de lo que nadie había imaginado.

Muchas organizaciones han tenido que adoptar nuevos modelos de operación con los que no están familiarizadas, además de implantar en poco tiempo tecnologías apropiadas para garantizar la continuidad del negocio en este nuevo entorno.

Las organizaciones están replanteándose el futuro. Para ello recomendamos centrarse en cinco áreas prioritarias: contención de costes, empoderamiento de los empleados, protección de las operaciones básicas, atención de las necesidades de los clientes y respuesta a cambios que afecten al portfolio de productos. La seguridad y la resiliencia operacional son fundamentales para satisfacer estas prioridades.

Algunos cambios recientes, como el auge del teletrabajo, conllevan mayores retos y amenazas de ciberseguridad para las organizaciones, ya que están más expuestas a los ataques. En muchos casos, la posición de riesgo ha variado de manera drástica. Este es el mejor momento para que redefina su estrategia de seguridad. En esta guía describimos algunos pasos que le ayudarán a conseguirlo, protegiendo las operaciones básicas de su negocio y garantizando la seguridad de sus empleados en este nuevo entorno de trabajo.

Los atacantes aprovechan que las organizaciones están más expuestas y, según un nuevo estudio de Microsoft, los hackers han lanzado ataques inspirados por el coronavirus en **241 países** y **territorios**

"... estos momentos de crisis son una oportunidad de redefinir nuestra forma de trabajar ... incluyendo la transformación de la empresa para mejorar aún más la experiencia del cliente y el nivel de eficiencia de las operaciones."

Centro de Investigación de Sistemas de Información del MIT Sloan
31 de marzo de 2020

La disrupción global **agrava** los problemas de seguridad

Son varios los desafíos de seguridad a los que tienen que hacer frente las organizaciones en esta nueva era:

Ingeniería social

Los ataques aprovechan el miedo a la crisis y utilizan cebos relacionados con la COVID-19 para lanzar campañas de phishing y malware. El número de estos ataques se ha incrementado de forma considerable y es probable que la tendencia se mantenga.

Teletrabajo

El aumento del teletrabajo ha traído consigo un incremento de los riesgos relacionados con la protección de dispositivos personales, contraseñas débiles, conexiones domésticas mal protegidas, routers y actualizaciones de sistemas remotos. Los empleados también están usando nuevas formas de colaboración dentro y fuera de la organización, a menudo a través de plataformas que son el blanco ideal para un ataque. Todo ello ha creado vulnerabilidades en herramientas de colaboración, lo que se traduce en una mala experiencia de usuario y problemas de privacidad y confidencialidad. Los líderes en seguridad tienen que afrontar costes de TI más elevados para dar soporte a la plantilla, así como un mayor uso de redes e infraestructuras.

Falta de acceso seguro

Los métodos de gobierno de identidades y accesos no se han adaptado a las nuevas formas de trabajo, incluyendo a trabajadores remotos, multitud de dispositivos y la imposibilidad de acceder a aplicaciones clave. La cantidad de información que se comparte también se ha multiplicado, lo que lleva a que muchas organizaciones se pregunten si disponen de la infraestructura y gobierno de identidad adecuados para que sus empleados y colaboradores puedan acceder de manera segura a la información que necesitan. El teletrabajo y los modelos de negocio remoto serán la nueva norma a partir de ahora. Los productos y servicios se intercambiarán en formato digital a través de la economía de las API, lo que aumentará todavía más la exposición a posibles ataques y los riesgos asociados

Falta de agilidad

El extraordinario aumento de la demanda de acceso remoto a recursos de las empresas supone una presión aún mayor para los puntos de acceso y los servicios de redes virtuales privadas (VPN). Muchas organizaciones no han podido adaptar de forma segura sus sistemas existentes e infraestructuras de VPN a las nuevas circunstancias, lo que está afectando a la experiencia del usuario y a su capacidad de trabajar.

> **Microsoft** detecta todos los días alrededor de **60.000** URL o archivos adjuntos **maliciosos** relacionados con el COVID-19

Sucesivas oleadas de cambio

Según nuestras previsiones, las organizaciones experimentarán tres oleadas de cambio. Es muy importante tomar las medidas de seguridad adecuadas para proteger las operaciones básicas del negocio y, de ese modo, crear una operación resiliente y escalable que esté preparada para un futuro flexible.

Respuesta

Muchas organizaciones ya están empezando a salir de esta primera fase. Para ello han tenido que centrarse en asegurar la continuidad del negocio, garantizando el trabajo de sus empleados y el acceso de los clientes a productos y servicios al tiempo que mantenían sus operaciones básicas y la cadena de suministro.

Es importante comprender cómo ha cambiado la posición de riesgo de la organización con el teletrabajo.

Reinicio

Cada vez es mayor el número de nuestros clientes que están dejando atrás la fase de respuesta para adoptar una mentalidad de reinicio, transformándose en empresas más ágiles y ligeras para hacer frente a la recesión económica. Es probable que para ello tengan que reconfigurar el portafolio de productos y crear con rapidez un modelo de negocio escalable que se adapte a las nuevas necesidades del mercado y los empleados.

Durante esta fase, recomendamos realizar una exhaustiva evaluación de riesgos para dar prioridad a la identificación de riesgos de seguridad, empezando por los problemas más inmediatos. También será necesario planificar un marco de seguridad basado en arquitecturas Zero-Trust y reducción de costes.

Renovación

En los próximos 12-18 meses, las organizaciones empezarán a plantearse cómo renovarse y crecer para posicionarse de cara al futuro. Su objetivo será reinventar el modelo de negocio para aprovechar oportunidades nuevas y existentes con una versión más fuerte y resistente de ellas mismas.

Desde el punto de vista de la seguridad, tendrán que adaptarse constantemente a las nuevas circunstancias sin dejar de cumplir las normas, de manera que todos los cambios de modelos, tecnología y procesos se ajusten a los nuevos requisitos normativos. También será el momento ideal para aplicar un nuevo diseño de seguridad basado en una estrategia y hoja de ruta sólida que responda los requisitos del negocio y a la posición de riesgo.

5 pasos para **redefinir** su estrategia de seguridad

A medida que vaya pasando por estas tres fases, tal vez le resulte difícil saber por dónde empezar para asegurarse de tomar las medidas adecuadas para proteger su empresa ahora y en el futuro.

A continuación, presentamos cinco pasos que pueden resultarle muy útiles.

#1. Adopte una mentalidad y una visión **Zero-Trust**

Este concepto se basa en el convencimiento de que una organización no debería confiar en nada de lo que haya dentro o fuera de sus límites, por lo que hay que comprobarlo todo antes de conceder el acceso a los sistemas. Debe haber un proceso de gobierno para verificar y gestionar la identidad de cada persona, cuenta de administración, aplicación, bot y proceso.

También le recomendamos el uso de herramientas de gobierno y administración de identidades (IGA, por sus siglas en inglés). El acceso a servicios digitales desde distintos lugares y plataformas se tiene que evaluar constantemente en función de los objetivos de resiliencia y continuidad de negocio.

avanade

Caso de éxito

Óptima seguridad para aprovechar todo el potencial del puesto de trabajo

Reto: Nuestro cliente deseaba crear un puesto de trabajo digital para el futuro e introducir una avanzada experiencia del empleado con una base segura.

Solución: Creamos un puesto de trabajo moderno y seguro basado en Microsoft 365 con una amplia gama de soluciones, desde servicios cloud seguros hasta un puesto de trabajo móvil y la colaboración más avanzada.

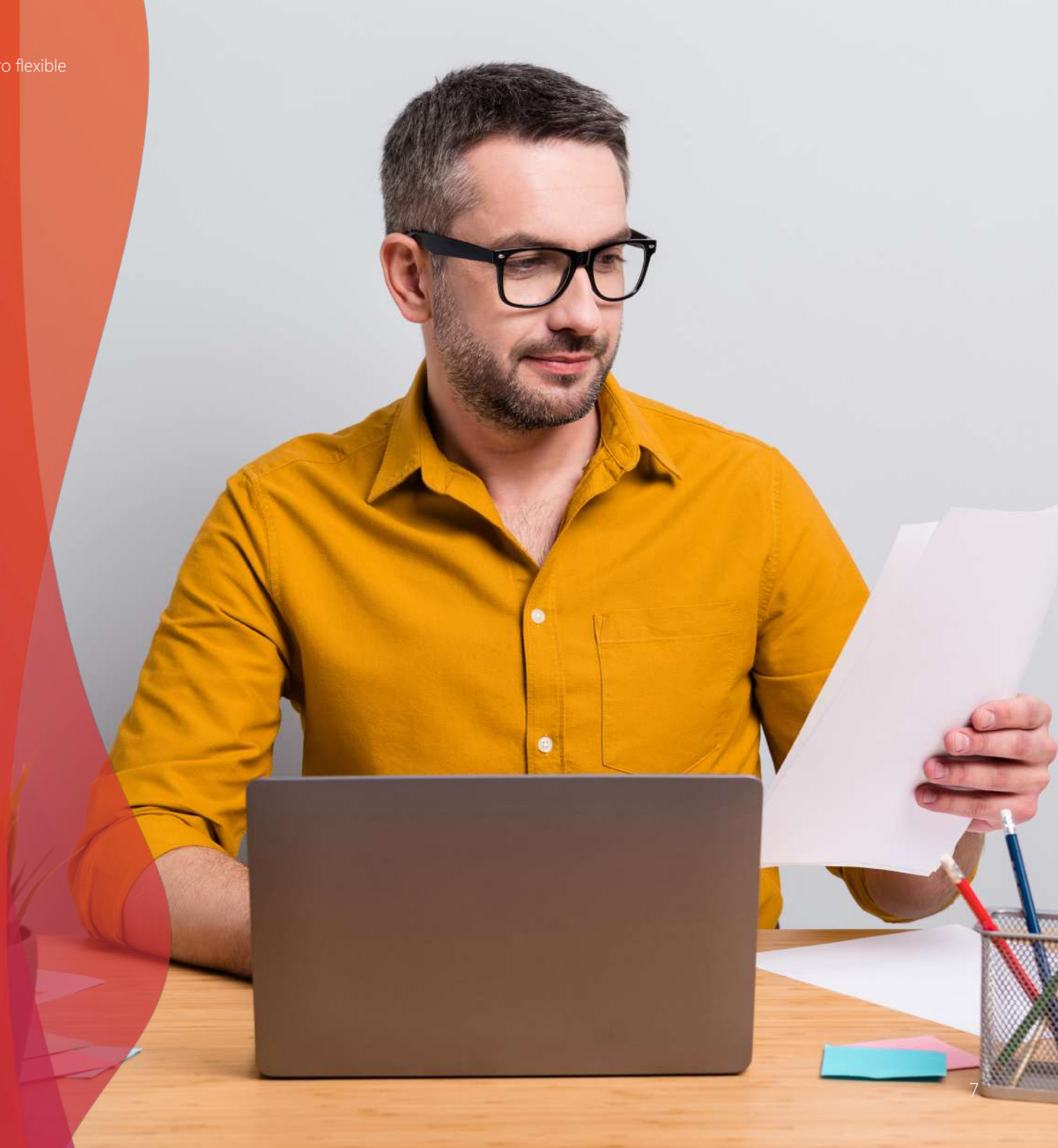
Resultados: El proyecto está ofreciendo excelentes resultados a la organización:

- Cumple dos principios básicos de **seguridad**: "Identidad como plano de control" y "Zero-Trust".
- Los empleados son más **productivos** y disfrutan de la misma experiencia de puesto de trabajo en distintos tipos de dispositivos de forma remota y segura.
- Las plataformas de puesto de trabajo seguras y en constante evolución han ayudado al cliente a llegar al mercado en menos tiempo y con más **eficiencia**.
- La **experiencia del empleado** ha mejorado mucho, con más colaboración y capacidad de tomar mejores decisiones.

#2. Realice una exhaustiva **evaluación de riesgos**

Si su organización, al igual que muchas otras, ha pasado recientemente por una fase de cambio rápido en la arquitectura empresarial y en la adopción de nuevas herramientas de trabajo y colaboración, ha llegado el momento de que realice una evaluación de riesgos de su entorno.

No es fácil evaluar el riesgo de todo desde el principio, así que le recomendamos empezar por identificar los activos que tienen más valor y comprender qué es lo que quiere proteger. Luego podrá identificar los riesgos más importantes para esos activos y desarrollar un plan táctico para contrarrestarlos.



avanade

#3. **Priorice** proyectos de seguridad, presupuestos y recursos

Conocer los riesgos en el nuevo ecosistema le permitirá adoptar un punto de vista más moderado y reflexivo a la hora de priorizar proyectos de seguridad, presupuestos y recursos.

También es un buen momento para desarrollar o renovar un marco formal de gobierno de la seguridad, de modo que su nuevo modelo operativo se ajuste a su nueva posición de riesgo.

Como la mayor parte de las cosas, la seguridad no es algo que se pueda garantizar solo con dinero. Un modelo basado en riesgos le ayudará a determinar su presupuesto y sus recursos. Muchos de nuestros clientes están dando prioridad al gasto en seguridad para proyectos de transformación digital y migración a cloud con el fin de facilitar el teletrabajo.

Según un estudio reciente de IDC, el gasto en servicios profesionales y gestionados relacionados con la seguridad seguirá siendo elevado, ya que las organizaciones tratarán de mantener sus operaciones en marcha durante la crisis del COVID-19. Esto demuestra la importancia de la seguridad como prioridad estratégica de las organizaciones, por delante de otras áreas de TI.

> IDC cree que el COVID-19 contribuirá a poner de relieve la importancia de contar con planes de resiliencia y respuesta a incidencias en situaciones de crisis.
>
> Impacto del COVID-19 en las previsiones de IDC para gasto en servicios de seguridad en 2020 [la fecha que figura en la página de IDC es 13 de abril de 2020

#4. **Simplifique** y **mejore** su entorno de seguridad

Es muy importante adoptar un modelo de seguridad por capas y con las herramientas adecuadas, pero sin dejar de buscar **oportunidades** de eliminar controles innecesarios.

Las arquitecturas de seguridad demasiado heterogéneas resultan difíciles de gestionar, son caras y pueden aumentar el riesgo de exposición, por lo que debe tratar de aprovechar capacidades que estén integradas en la plataforma de su proveedor cloud.

Eso le será especialmente útil si tiene que reaccionar con rapidez a una situación como el teletrabajo. Asegúrese de sacar el máximo partido a las capacidades de seguridad integradas, como las que incluye Microsoft 365, para reducir costes innecesarios.

avanade

#5. **Renueve** para hacer realidad su visión de la seguridad a largo plazo

Le recomendamos adoptar una visión integral de la seguridad y convertirla desde el principio en parte de la transformación digital de su organización.

Integre la seguridad en las aplicaciones y soluciones de TI, en lugar de recurrir a soluciones de moda que pronto pueden pasar a ser redundantes.

Sean como sean sus sistemas, haga que sean seguros desde la perspectiva cloud y las aplicaciones modernas. Asegúrese de comprender cuál es el grado de responsabilidad del proveedor (y el tuyo propio) para garantizar su seguridad por diseño.

La seguridad tiene que ser un catalizador de negocio. Busque un equilibrio entre seguridad y controles para no añadir barreras que reduzcan la productividad de los empleados. De este modo, su organización funcionará con agilidad y estará preparada para lo que nos depare el futuro.

Por último, de prioridad a fomentar una fuerte cultura de seguridad. Una formación sólida en seguridad le ayudará a hacer frente a los riesgos de seguridad inherentes al comportamiento de los empleados. Es posible que para ello necesites un modelo de gestión del cambio respaldado por actividades y formación continua de los empleados según su rol.

avanade

¿Por qué **Avanade**?

Para liderar el mercado actual hay que pensar de fuera adentro

En Avanade seguimos ayudando a nuestros clientes en estos difíciles momentos. Desde que se inició la pandemia de COVID-19, hemos migrado más de un millón de cuentas de teletrabajo para nuestros clientes. Ahora estamos guiando a esas organizaciones hacia un modelo operativo seguro y con capacidad de adaptarse para protegerlas en el futuro.

Somos expertos en protección de ecosistemas de TI basados en Microsoft o híbridos. Nuestros servicios de seguridad ofrecen una solución integral que incluye asesoramiento, implementación y servicios gestionados. Podemos ayudarle a realizar una evaluación de riesgos e implantar una arquitectura de seguridad. Como proveedores de seguridad gestionada, también podemos extender su equipo de seguridad con monitorización permanente de eventos y soporte operativo constante para que pueda adelantarse a cualquier riesgo de seguridad.

Ofrecemos metodologías de eficacia probada, profundos conocimientos y la tecnología más avanzada. Por algo llevamos 14 años siendo elegidos Partner del año de Microsoft en integración de sistemas.

AVANADE IS GOLD FOR MICROSOFT'S SECURITY COMPETENCY

MICROSOFT SECURITY 20/20 SECURITY ADVISORY OF THE YEAR WINNER

MICROSOFT PARTNER FOR OFFICE 365 FOR TEN CONSECUTIVE YEARS

MICROSOFT ALLIANCE PARTNER OF THE YEAR FOR 14 YEARS

avanade

Empiece **hoy mismo**

Muchos clientes han tenido que adaptarse en muy poco tiempo al teletrabajo. Si ese es su caso, puede empezar con nuestras actividades de evaluación de nivel de seguridad y taller.

Trabajaremos con usted para comprender su situación, infraestructura y procesos para que pueda llevar a cabo una evaluación integral del entorno de seguridad y construir una hoja de ruta que haga realidad su visión de la seguridad a largo plazo.

Ponemos a su disposición las siguientes opciones:

Evaluación de seguridad y taller de Microsoft 365

- Evaluamos su actual entorno de Microsoft 365 desde el punto de vista de la seguridad para identificar espacios no cubiertos y áreas de remediación.
- Realizamos un completo análisis y recomendamos una estrategia basada en los controles de seguridad y los requisitos de negocio de su organización.
- Un informe de puntuación de seguridad y un dashboard que proporcionan detalles sobre gobierno y protección de información.
- Una evaluación integral que proporciona orientación para mitigar los riesgos de ciberseguridad en evolución.

Evaluación de infraestructuras de identidades y procesos

- Realizamos una completa evaluación y descubrimiento automatizado de riesgos.
- Evaluamos su infraestructura para recomendar posibles mejoras.

Póngase en contacto con nosotros si quiere más información o visite **nuestra página dedicada a Seguridad.**

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

Sobre Avanade

Avanade es el proveedor líder de innovadores servicios digitales y cloud, soluciones de negocio y experiencias de diseño en el ecosistema de Microsoft. Con 38 000 profesionales en 25 países, somos la fuerza que impulsa el Accenture Microsoft Business Group para ayudar a las empresas a atraer clientes, potenciar a sus empleados, optimizar operaciones y transformar productos empleando la plataforma de Microsoft. Con participación mayoritaria de Accenture, Avanade fue creada en el 2000 por Accenture LLP y Microsoft Corporation. Más información en www.avanade.com.

avanade


avanade